Government Brief

Data Protection for Physical, Virtual, and Cloud Environments

Enterprise Encryption and Key Management Simplified

Vormetric

Overview

On Monday July 8th, 2012 US National Security Agency (NSA) Chief Keith Alexander described the state of cyber security in the US while speaking to the American Enterprise Institute event in Washington, D.C. Referencing public and classified sources, Mr. Alexander stated that *"…for every company that knows it has been hacked, another 100 do not know their systems have been breached."* According to the NSA, breaches increased 44% between 2010 and 2011 alone. Mr. Alexander then informed the crowd that there are now *"…75 million unique pieces of malware on the loose."* For companies tasked with protecting sensitive data, these statements reinforced what most already knew.

It goes without saying that companies are facing increasingly difficult challenges in the protection of sensitive data. In 2012, the US Government, along with the Ponemon Institute, conducted a survey intended to gauge the effectiveness of current security measures and to estimate the cost of increasing the measures to achieve 95% security. The results were disheartening. The survey of 172 organizations across 6 industries revealed that companies are currently only achieving an average of 68% effective security while spending an average of $42 million per year on security. The survey evaluated the three standard network-centric security components of:

1. Attack prevention
2. Attack detection
3. False positive rates

To achieve an "optimal" security posture of 95%, companies would need to increase security spending an average of 900% annually, with some industries requiring a 1,200% increase in spending. Increasing spending 9 fold is not realistic for any company or industry. To add to the frustration, the report demonstrates diminishing returns on security expenditure.

Currently, financial services organizations are, according to the survey, achieving 68.67% security with an average of $22 million spent annually. To achieve 80.33% the company must, according to the report, increase spending an additional $44 million for a total of $66 million per year. For every 1% increase in security the company must allocate an additional $3.77 million in security. This demonstrates the inherent inefficiencies of the current network centric security model. Quite simply, something must change.

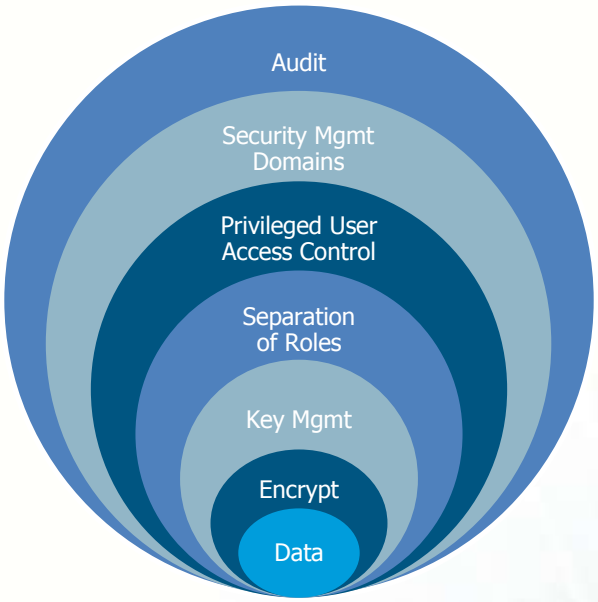
Key Technology Enabler

Our customers view Vormetric as a Key Data Security Technology Enabler. In the past, companies had the luxury of allocating budgets to allow physical separation of data for different groups or different data classification levels. Often servers were only running at 5-20% utilization as they were dedicated to specific types of data. This inefficient allocation of resources is no longer feasible in light of the information above, as well as the tightening of IT budgets as companies face increasingly difficult economic times. In light of the Ponemon survey it is clear that companies must find ways to operate more efficiently and more effectively with regard to security.

So how does a company operate more efficiently AND effectively in today's environment? One way is by employing a layered security approach. Traditional models of data protection focused largely on network-centric security, while an improvement, these have proven to be most effective when coupled with a data-centric protection strategy. Investing in more network devices such as firewalls, intrusion detections systems, and more robust segmentation is important, but by creating a layered approach that includes proven, robust encryption, key management, and access controls, companies can improve their security posture much more effectively and efficiently than by solely focusing on the network security. Encryption works in concert with technologies such as DLP and database monitor provides a comprehensive multi-layered approach to protecting the sensitive data.

Data Centric Approach

Strong encryption algorithms approach mathematical impossibility to crack through existing computational methods. So where is the proverbial weak link? Quite simply, the three areas that create weaknesses in many encryption implementations are key management and access control. First, if encryption keys are not sufficiently protected, they are vulnerable to theft by malicious hackers. It is paramount that any encryption implementation has a robust key management solution to provide assurance that the keys are sufficiently protected from compromise. The second vulnerability lies in the access control model. If keys are appropriately protected but access is not sufficiently controlled or robust, malicious personnel can attempt to access sensitive data by assuming the identity of an authorized user. An additional weakness lies in the auditing of file access. Organizations are well advised, not only to monitor file access, but specifically to audit the entire encryption and key management solution. For this reason, it is critical that any data centric approach include encryption, key management, robust access controls and file monitoring.



Vormetric and the US Intelligence Community

Vormetric combines industry leading encryption, key management, and access control to protect sensitive data. Additionally, by leveraging expertise gathered through a unique partnership with the US intelligence community, Vormetric is able to provide a "chain of custody" on sensitive data. For the first time, data with different classification levels are allowed to reside on the same physical disk. By consolidating data with different classification levels onto the same device, companies reduce infrastructure complexity, and increase efficiency by allowing systems to operate at much higher capacities than the traditional 5%-20%. Robust access controls provide assurance that only authorized users and applications can access the data. Vormetric supports the ability to create "zones of encryption". These administrative zones or domains are logical partitions that can be used to separate administrators, and the data they secure, from other administrators. Administrative tasks are performed in each domain based upon each administrator's assigned type. The advantages of administrative domains are:

- Leveraging the Vormetric Data Security environment and investment
- Segregation of data for increased security
- Separation of responsibilities
- No one administrator has complete control of the protected data

Consider a traditional environment with data in three different classification levels. In current models, each classification level would require three separate disks to house the data, and would require complex access control mechanisms, and three different encryption implementations. This model is not only inefficient, but the increased complexity of the solution provides opportunities for multiple points of failure. If classification levels can be consolidated, there is the potential for large operational and economical gains. In addition, Vormetric offers many layers of redundancy to support customers who require near 100% uptime. Fortune 100 companies lose hundreds of thousands of dollars per hour when their systems are down and with government clients, lives may be lost if systems fail. By reducing complexity, and potentially the points of failure, Vormetric minimizes the opportunity for downtime.

Vormetric, Inc.
888.267.3727
Sales@vormetic.com
Vormetric.com